AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information associated with yuzhou414@gmail.com that is stored at premises controlled by Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043

Case No. 2:18 mj 490

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE THE ATTACHED AFFIDAVIT IN SUPPORT OF THIS APPLICATION, AND ATTACHMENT A THERETO IN PARTICULAR, ALL OF WHICH IS INCORPORATED HEREIN BY REFERENCE.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

SEE THE ATTACHED AFFIDAVIT IN SUPPORT OF THIS APPLICATION, AND ATTACHMENT B THERETO IN PARTICULAR, ALL OF WHICH IS INCORPORATED HEREIN BY REFERENCE.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section		*Offense Description*
18 U.S.C. 1832		Theft of Trade Secrets

The application is based on these facts:

See attached affidavit incorporated herein by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Steven E. McCann, SA FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: June 26, 2018

Judge's signature

City and state: Columbus, Ohio

Kimberly A. Jolson, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF OHIO

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

In the matter of the search of information associated with yuzhou414@gmail.com that is stored at premises controlled by Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043	Case No. 2:18mj490 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Steven E. McCann, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION

1. As set forth in detail below, an investigation into the theft of trade secrets (intellectual property and proprietary research data) from Nationwide Children's Hospital (NCH), specifically by two former NCH employees, Yu Zhou and Li Chen, has been ongoing since January 2018. The facts herein establish probable cause to believe Yu Zhou and Li Chen conspired with each other to steal trade secrets belonging to NCH, their former employer, in violation of Title 18 U.S.C. § 1832, Theft of Trade Secrets.

2. Relevant here, I make this affidavit in support of applications for a search warrant for information associated with each of the below-listed accounts (the Subject Accounts) that is stored at premises controlled by Google, Inc. (Google or the Provider), an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043, believing evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1832 are located within said Subject Accounts. The property or information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search

warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google, Inc. to disclose to the United States copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. The Subject Accounts are as follows:

A. The email account yuzhou414@gmail.com (Subject Acccount-1), created on or about 07/22/2011, subscribed to by Yu Zhou with recovery email address Genexosome@163.com, which account is maintained at premises controlled by Google, a company headquartered in Mountain View, California.

B. The email account chenliandzhouyu@gmail.com (Subject Account-2), created on or about 09/15/2011, subscribed to by Li Chen with recovery email address Genexosome@163.com, which is maintained at premises controlled by Google, a company headquartered in Mountain View, California.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

II. AGENT BACKGROUND

5. I have been employed as a Special Agent of the Federal Bureau of Investigation (FBI) since March 2008, and I am currently assigned to the Cincinnati Division, Columbus Resident Agency, as a member of the Counterintelligence Squad. I am responsible for investigating, among other crimes, the theft of trade secrets. I have received both formal and informal training in the detection and investigation of said offense. As a result of my training and experience, I am familiar with the federal laws relating to the theft of trade secrets. I have participated in various investigations, including those with a foreign counterintelligence nexus. As a federal agent, I am authorized to investigate violations of the laws of the United States.

6. I have personally participated in the investigation described herein. I have reviewed the relevant documents and reports of witness interviews during the course of this investigation. The statements contained in this affidavit are based on my own observations, document reviews, and reliable information provided to me by other law enforcement officials. Because this affidavit is being submitted for the limited purpose of establishing probable cause to search the Subject Accounts described below, I have not included each and every fact learned during the course of this investigation. Rather, I have set forth those facts that I believe are necessary to establish probable cause for the search warrant sought. Where actions, conversations, and statements of others are related, they are related in part, except where otherwise indicated.

7. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. § 1832 have been committed by Yu Zhou and Li Chen. There is also probable cause to believe that fruits, evidence, and instrumentalities of these crimes in the form of electronic communications, as described in Attachment B, are located at the internet service provider, as described in Attachment A.

III. JURISDICTION

8. Pursuant to 18 U.S.C. § 2703(a), (b)(1)(A) & (c)(1)(A), the United States may require a provider of an electronic communications service or remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information pertaining to subscribers, by obtaining a warrant issued using the procedures described in Federal Rule of Criminal Procedure 41.

9. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A) &

(c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

IV. APPLICABLE STATUTES AND DEFINITIONS

10. Since January 2018 to the present, the FBI has been investigating Yu Zhou and Li Chen for violations of 18 U.S.C. § 1832, and the investigation has determined that there is probable cause to believe that violations of U.S. laws have occurred.

11. I am advised that 18 U.S.C. § 1832 provides in relevant part:

> (a) Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—
>
> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;
>
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
>
> . . . .
>
> shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

12. I am further advised that the term "trade secret" is defined by 18 U.S.C. § 1839(3) as follows:

> [T]he term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
>
> (A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

13. I am further advised that the elements of a violation of 18 U.S.C. § 1832 are: (a) the defendant intended to convert a trade secret to the economic benefit of anyone other than the owner; (b) the information was, in fact, a trade secret; (c) the defendant knowingly stole, or without authorization appropriated, took, carried away, or concealed, or by fraud, artifice, or deception obtained the trade secret; (d) the defendant intended, or knew, the offense would injure the owner of the trade secret; and (e) the trade secret was related to or included in a product that is produced for or placed in interstate or foreign commerce. *See* 18 U.S.C. § 1832(a)(1); *see also United States v. Howley*, 707 F.3d 575, 579 (6th Cir. 2013); *United States v. Hsu*, 155 F.3d 189, 195–96 (3d Cir. 1998).

V. BACKGROUND INFORMATION REGARDING EMAIL AND GOOGLE

14. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail (email) access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com, like the email Subject Accounts. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

15. In addition to emails, a Google subscriber can also store files with provider, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

16. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

17. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the particular provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address (IP address) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address

information can help to identify which computers or other devices were used to access the email account.

18. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

19. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contact lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the IP addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and

geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Stored electronic data might also provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

20. Google Plus (stylized as Google+) is an internet-based social network owned and operated by Google. The following paragraphs detail the features and functions associated with Google Plus social networking accounts.

A. User Profile: A Google Plus user profile is a publicly visible account of a user that is attached to many Google properties. The user profile includes basic social networking services like a profile photo, about section, background photo, cover photo, previous work and school history, interests, places lived and an area to post status updates.

B. Circles: Circles enables a user to organize people into groups or lists for sharing across various Google products and services. Organization of Circles is done through a "drag and drop" interface. Once a Circle is created, a Google Plus user can share specific private content to only that circle.

C. Stream: Within the Stream section, Google Plus users see updates from those in their Circles. There is an input box which allows users to enter a post. Along with the text field there are icons to upload and share photos and videos.

D. Privacy: The privacy setting allows Google Plus users to disclose certain information to the circles of their choice. Users can also see their profile visitors.

21. Google Plus also retains IP logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Google Plus, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Google Plus profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

22. Social networking providers like Google Plus typically retain additional information about their user's accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Google Plus users may communicate directly with Google about issues relating to their account(s), such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Google Plus typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communication.

23. Therefore, the computers of Google are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Google Plus, such as account access information, transaction information, and account application.

24. Google Drive is a file storage and synchronization service developed by Google. Google Drive allows users to store files on their servers, synchronize files across devices and share files. Google Drive offers users 15 gigabytes of free storage with virtually unlimited storage space through an optional paid plan. Digital files uploaded can be up to 5 terabytes in size.

25. Google Drive users have the ability to upload any digital file to Google Drive for data retention and data backup. Google Drive users have the ability to access content from their Google Drive account from any device connected to the internet, including computers, tablets, Android smartphones or iPhones.

26. Based on training and experience, Gmail, Google Plus, and Google Drive, as well as other Google products, can all be backed up and synchronized with each other. The back-up and synchronization process creates additional copies of digital files in multiple locations for ease of access and to secure data from accidental deletion.

27. This application seeks a warrant to search all responsive records and information under the control of Google, which is a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The United States intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

VI. INVESTIGATION AND PROBABLE CAUSE

A. Relevant Individuals and Entities

28. Yu Zhou (ZHOU) is a naturalized U.S. Citizen, the co-founder and CEO of GENEXOSOME TECHNOLOGIES, INC., and a former employee of Nationwide Children's Hospital (NCH), which is located in Columbus, Ohio. ZHOU worked for NCH as a researcher in the lab of Dr. Gail Besner. Dr. Besner's lab was focused on, among other topics, the research of exosomes (which are described in more detail below), and specifically with respect to intestinal

issues in premature infants. ZHOU was the longest tenured lab member until he resigned in 2017. He worked in Dr. Besner's lab from 2007 until 2017. ZHOU is the spouse of Li Chen.

29. Li Chen (CHEN) is a naturalized U.S. Citizen and former employee of NCH. CHEN worked for NCH as a researcher in the lab of Dr. David Brigstock. Dr. Brigstock's lab was focused on, among other topics, the research of exosomes with respect to liver fibrosis. CHEN resigned from NCH in 2018. CHEN worked at NCH from 2008 until 2018. CHEN is the spouse of ZHOU.

30. During ZHOU's and CHEN's tenures, both Dr. Besner's and Dr. Brigstock's respective labs focused on and utilized scientific developments with respect to exosomes in research. An October 30, 2017, press release regarding Avalon GloboCare Corp., Beijing Jiteng Biotechnology Co. LTD., and Genexosome Technologies, Inc., which are three of the entities related to this warrant application, defines exosomes as: "tiny, subcellular, membrane-bound vesicles[] measur[ing] 30-150 nm in diameter that are released by almost all cell types." The press release further notes that "[e]xosomes can carry membraned and cellular proteins, as well as genetic materials that are representative of cell origin. Profiling various bio-molecules in exosomes may serve as useful biomarkers for a wide variety of diseases."

31. Beijing Jiteng Biotechnology Co. LTD. (BEIJING GENEXOSOME) is a Limited Liability Corporation established in Beijing, China in 2015 by ZHOU and CHEN. According to a press release from October 2017, and to corresponding Securities and Exchange Commission filings, BEIJING GENEXOSOME is engaged in the development of exosome technology to improve diagnosis and management of diseases. BEIJING GENEXOSOME produces research kits that are designed to be used by researchers for biomarker discovery and clinical diagnostic development, as well as for the advancement of targeted therapies. Currently, BEIJING

GENEXOSOME's research kits and services are available for purchase, and the kits can be used to isolate exosomes or extract exosomal RNA/protein from serum/plasma, urine and saliva samples. These research kits are advertised to increase the yield and purity of such samples, as well as to isolate exosomes with intact membranes. This is important, especially in the research of diseases affecting premature babies, where the sample sizes are extremely small in volume. As part of its business, BEIJING GENEXOSOME is also seeking to decode proteomic and genomic alterations underlying a wide range of pathologies, thus allowing for the introduction of novel, non-invasive "liquid biopsies." Its mission is focused toward diagnostic advancements in the fields of oncology, infectious diseases and fibrotic diseases, and discovery of disease-specific exosomes, all of which would provide disease-origin insight necessary to enable personalized clinical management.

32. ZHOU is the Chief Executive Officer (CEO) of GENEXOSOME TECHNOLOGIES, INC. (GENEXOSOME TECH). GENEXOSOME TECH is a Foreign For-Profit Corporation according to State of Ohio business records. State of Ohio business records also indicate that, in November 2017, ZHOU registered GENEXOSOME TECH at the following addresses: a principal office located at 4400 Route 9 South, Suite 3100, Freehold, New Jersey 07728, and an Ohio office located at 168 Dorchester Square, Suite 101, Westerville, Ohio 43081. GENEXOSOME TECH's website indicates that the company is a leading biotechnology company focused on the development of exosome-based diagnostic and therapeutic products. Also, according to GENEXOSOME TECH's website, the company was co-founded in the United States by Avalon GloboCare Corp. and Dr. Yu Zhou, a clinical scientist who has spent more than 10 years on exosome research and clinical utilization of exosomes products. The website further states that their proprietary Exosome Isolation System has proven to be a cutting-edge technology,

as it greatly enhances exosome isolation efficiency and exosome quality. The company, according to the website, also develops proprietary exosome isolation systems, promotes implementation of exosome biotechnology in "liquid biopsy" and targeted therapies, and provides the global market with innovative exosome products for clinical diagnosis and treatment. Furthermore, GENEXOSOME's website states it has U.S. operations in New Jersey and Ohio, in addition to overseas operations in Beijing, Shanghai and Wuhan in China.

33. BEIJEING GENOXOSOME and GENEXOSOME TECH are related entities. Avalon GloboCare Corp. (AVALON) is a U.S. Corporation based out of Freehold, New Jersey. According to AVALON's website, the company is a premiere healthcare management provider and biotechnology developer, dedicated to integrating and managing global healthcare resources, empowering high-impact biomedical innovation and technologies, as well as to engaging in bio-venture investment. The co-founder and current CEO of AVALON is Dr. David Jin. According to the State of Nevada business records, AVALON formed GENEXOSOME TECH in July 2017. This GENEXOSOME TECH is the same entity described in the previous paragraph. The records further indicate Dr. David Jin as the CEO of GENEXOSOME TECH. According to information contained in a press release from October 2017, AVALON announced that its majority-owned subsidiary, GENEXOSOME TECH, acquired 100% of the outstanding capital stock of BEIJING GENEXOSOME. Concurrently, GENEXOSOME entered into and closed an Asset Purchase Agreement with ZHOU, CEO of BEIJING GENEXOSOME, pursuant to which GENEXOSOME TECH acquired all assets, including intellectual property, patents and patent applications held by ZHOU pertaining to the business of researching, developing and commercializing exosome technologies.

B. Facts Establishing Probable Cause: Yu Zhou, Li Chen and GENEXOSOME TECH

34. In the month following ZHOU's departure from NCH, multiple wire transfers were made from AVALON to ZHOU and CHEN's personal Chase bank account. The notable wire transfers are as follows:

A. On or about 11/20/2017, AVALON transferred $499,000 to ZHOU and CHEN's Chase account;

B. On or about 11/21/2017, AVALON transferred $200,000 to ZHOU and CHEN's Chase account;

C. On or about 11/23/2017, AVALON transferred $100,000 to ZHOU and CHEN's Chase account; and

D. On or about 11/27/2017, AVALON transferred $77,087 to ZHOU and CHEN's Chase account.

35. In the month before receiving the above wire transfers, on or about October 8, 2017, ZHOU emailed his resignation to Dr. Besner, effective on or about November 10, 2017, with his last physical day in the lab being on or about October 27, 2017. This email was sent to Dr. Besner from ZHOU's NCH email account, Yu.Zhou@nationwidechildrens.org.

36. In or around November 2017, NCH received an anonymous letter regarding the potential theft of intellectual property, misconduct and conflict of interest by two NCH employees, ZHOU and CHEN. The letter describes ZHOU as a research scientist in the lab of Dr. Besner, as well as being the CEO of GENEXOSOME TECH. The letter further describes CHEN as a research associate in Dr. Brigstock's lab. Furthermore, the letter addresses the fact that ZHOU and CHEN filed four patents in the People's Republic of China (PRC) on topics related to exosomes, miRNA, and liver diseases, all similar topics as those developed and researched in their respective NCH labs. The letter also described the selling of those four patents and all related intellectual property

from BEIJING GENEXOSOME to AVALON and its now-U.S. subsidiary, GENEXOSOME TECH.

37. The investigation to date has revealed that Dr. Besner, in her research lab at NCH, has developed a method for isolating exosomes from very tiny samples and then purifying those samples for research. Based on interviews of Dr. Besner, this method was borne out of necessity, given the fact that she works with and conducts research on premature babies and is unable to obtain large bodily fluid samples. This information has never been presented in a public forum and has not been published. Dr. Besner considers this method to be proprietary to her lab and NCH property. A review of the GENEXOSOME TECH website reveals a product for sale, called the "GET™ Exosome Isolation Kit." In a publicly available Avalon GloboCare press release, dated October 30, 2017, ZHOU discusses a proprietary exosome isolation system, where represents that he is able to capture exosomes from a tiny volume of bodily fluid. This product is similar to the method developed by Dr. Besner in her lab at NCH.

C. Reasonable Measures to Protect Information

38. Given the value placed on this research and information, NCH has taken reasonable measures to protect the information from unauthorized parties outside of the hospital. For example, NCH has placed the information on private servers, required badge access to research labs and required annual training regarding the protection of its information.

39. To ensure employees are aware of NCH Policies and Procedures (P&P), NCH has employees review and sign an "Employee Handbook Acknowledgement" document during new-employee onboarding. The employee handbook refers to all NCH P&P, and by signing the handbook the employee acknowledges that she or he will be bound by all NCH policies. All NCH policies are available at any time online to all employees. In addition, NCH has new employees

review and sign several other documents, to include: 1) Nationwide Children's Hospital, Inc. Confidentiality and Security Agreement; and 2) Certification Related To Nationwide Children's Corporate Integrity Program. ZHOU signed these documents on February 26, 2007 and CHEN signed these documents on January 8, 2008.

40. NCH reinforced the importance of safeguarding and protecting this information was through initial and periodic training, to include, but not limited to: "Case Study – Data Management 'Who Owns Research Data?'," and "Responsible Conduct of Research (RCR) Course Introduction and Research Misconduct," which ZHOU and CHEN both completed. NCH also has a banner on their computers notifying all employees that NCH is allowed to monitor all employee computer activity. The banner reads as follows:

> A. This is a restricted network. Any person or system gaining unauthorized access will be subject to prosecution. Nationwide Children's Hospital, Inc. computer systems are to be used for business purposes only. Nationwide Children's Hospital Inc., reserves the right to monitor, audit and investigate any inappropriate use of its systems. Unauthorized or improper use of this system may result in administrative disciplinary action and or civil or criminal penalties. By continuing to use this system you indicate your awareness of and consent to the Terms and conditions of use. Discontinue use of this computer immediately if you do not agree to the conditions stated in this warning.

D. Use of External Email Accounts

41. The investigation to date has also revealed that, as of May 23, 2018, ZHOU and CHEN forwarded at least 30 emails to and/or from their NCH email accounts to multiple external email accounts. Those accounts are as follows: yuzhou414@gmail.com, chenliandzhouyu@gmail.com, joe@genexo-tech.com and genexosome@163.com. The latter two email accounts, joe@genexo-tech.com and genexosome@163.com, are hosted overseas on servers located in China. Relevant to this affidavit, the representative examples below demonstrate that

ZHOU and CHEN sent and received emails from and to the Subject Accounts regarding NCH, GENEXOSOME TECH, and matters related to exosomes.

42. On or about February 8, 2017, CHEN emailed chenliandzhouyu@gmail.com an email with two attachments. The attachments were labeled: "Biogenesis and secretion of exosomes.pdf" and "Biogenesis, Secretion, and Intercellular Interactions of exosomes and other Extracellular Vesicles.pdf." CHEN utilized her NCH email account, Li.Chen@nationwidechildrens.org, to send this information. Based on interviews/investigation to date, NCH did consider and still considers the information in these attachments confidential and proprietary.

43. On or about July 14, 2017, CHEN utilized her NCH email account, Li.Chen@nationwidechildrens.org, to email chenliandzhouyu@gmail.com, copying yuzhou44@gmail.com. The email attached a Word document quoting language from NCH policy concern the ownership of intellectual property. The language included the following provisions:

A. "As stated in the hospital policy, all technical discoveries, inventions, and non-academic work authored, developed, or invented by any person employed by Nationwide Children's Hospital, Inc. or its subsidiaries or by those using its facilities, is considered property of the hospital. An inventor is defined as any member of the medical staff of Nationwide Children's Hospital and/or OSU faculty member using the facilities at Nationwide Children's Hospital. This definition also encompasses all employees of Nationwide Children's Hospital during their regular course of employment, those engaged in activities involving research or clinical investigation, all house staff, appointees, professional students, consultants and other personnel engaged in basic or applied research, testing activities or service programs at the institution."

B. "Patents and copyrights issued or acquired as a result of or in connection with administration, research, or other educational activities conducted by members of Nationwide Children's Hospital, Inc. and supported directly or indirectly by funds administered by Nationwide Children's Hospital, Inc. or The Research Institute at Nationwide Children's Hospital, regardless of the source of such funds, and all royalties or other revenues derived therefrom shall be the property of Nationwide Children's Hospital, Inc.

> Nationwide Children's Hospital, Inc. reserves the right to retain, assign, license, transfer, sell or otherwise dispose of, in whole or in part, any and all rights to, interests in, or income from any such discoveries, inventions or patents, except in cases of sponsored research projects where the terms of the research contract specifically require the assignment of patent or other rights to the sponsor."

44. On or about August 24, 2017, CHEN emailed genexosome@163.com an email with a PowerPoint presentation attached named "Figure-myography.pptx." CHEN utilized her NCH email account, Li.Chen@nationwidechildrens.org, to send this information. Based on interviews/investigation to date, this attachment is identified as a graph depicting the analysis of research data, all of which NCH did consider and still considers confidential and proprietary.

45. On or about August 25, 2017, CHEN sent chenliandzhouyu@gmail.com an email with an attachment labeled, "recommendation letter (Dr. David Jin).docx." CHEN utilized her NCH email account, Li.Chen@nationwidechildrens.org, to send this email.

46. On or about August 25, 2017, ZHOU sent chenliandzhouyu@gmail.com an email with the subject line of "Fw: weekly update" and an attachment labeled, "Figure-myography.pptx." ZHOU utilized his NCH email account, Yu.Zhou@nationwidechildrens.com, to send this email.

47. On or about November 20, 2017, CHEN emailed joe@genexo-tech.com an email with a subject line of "report of XY test" and an attachment labeled "XY1 test 2017-11-20 15-40-00-ExperimentReport.pdf." CHEN utilized her NCH email account, Li.Chen@nationwidechildrens.org, to send this email. Based on interviews/investigation to date, this attachment is identified as a report of test results regarding male mice in the lab of Dr. Brigstock. NCH did consider and still considers this research data to be confidential and proprietary.

48. On or about November 21, 2017, CHEN emailed joe@genexo-tech.com an email with a subject line of "TEM" and it included four attachments labeled: "sample 1 45k-1.tif,"

"sample 2 50k-1.tif," "sample 5 50k-4.tif," and "sample 5 50k-5.tif." CHEN utilized her NCH email account, Li.Chen@nationwidechildrens.org, to forward this information. Based on interviews/investigation to date, these attachments are identified as images of exosomes. These images are part of a larger research data set that is currently ongoing at NCH, has not yet been published or made public, and was funded by NIH grants. NCH did consider and still considers this information confidential and proprietary.

E. Summary

49. The above referenced attachments include images of exosomes captured utilizing highly sophisticated, scientific equipment belonging to NCH, as well as graphs, charts and documents depicting exosomes, to include analysis of ongoing or past research, all funded by National Institutes of Health (NIH) grants, with work being conducted on NCH property and with NCH resources.

50. Images and research data similar to those sent as attachments in the above referenced emails have appeared on marketing materials for GENEXOSOME TECH products. The referenced product marketing materials are publicly available on the GENEXOSOME TECH website.

51. The above identified emails and each of their accompanying attachments pertain to the same subject areas as the work being conducted by GENEXOSOME TECH, as well as the products GENEXOSOME TECH markets and sells. The information identified in several of the email attachments is proprietary and highly marketable scientific information developed and derived from NIH grant funding at NCH. The emails, as well as the above information regarding BEIJING GENEXOSOME and GENEXOSOME TECH, and the payments to ZHOU and CHEN, provide probable cause that ZHOU and CHEN took this proprietary information from NCH with

the intention of profiting from such information in the creation and sales of related and derivative products.

52. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the Provider's servers associated with the Subject Accounts will contain evidence, fruits, and instrumentalities of the Subject Offense, 18 U.S.C. § 1832, as more fully described in Section II of Attachment B.

53. In particular, I believe the Subject Accounts are likely to contain, among other things, the following information:

A. Evidence of the identity or identities of the user(s) of the Subject Accounts;

B. Evidence of downloading, replicating, transmitting, or delivering research conducted at NCH to personal email accounts;

C. Evidence of the identities and locations of co-conspirators in the Subject Offense, including photographs, images, and communications with such individuals;

D. Evidence of participation in the Subject Offense by the user(s) of the Subject Accounts and others, including records relating to financial transactions in furtherance of the Subject Offense; and

E. Evidence related to banks and other financial institutions at which the user(s) of the Subject Accounts conduct business, including potential transactions in furtherance of the Subject Offense.

VII. CONCLUSION

54. The evidence stated herein establishes probable cause to believe that ZHOU and CHEN have violated U.S. law regarding Title 18 U.S.C. § 1832, Theft of Trade Secrets. There is further probable cause to believe that evidence, fruits, and instrumentalities of this crime will be found on the premises of Google Inc., as described above and attached. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on

Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

VIII. REQUEST FOR SEALING

55. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, tamper with or destroy evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

Steven E. McCann
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on June 26, 2018

Honorable Kimberly A. Jolson
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with yuzhou414@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google, Inc., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Google

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Inc., regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Google, Inc., or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the United States for each account or identifier listed in Attachment A. Such information should include the below-described content of the Subject Accounts() from January 1, 2015 to the present.

1. The contents of all emails, opened or unopened, associated with the Subject Accounts, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
2. Any deleted emails, including any information described in subparagraph "1." above;
3. All records or other information regarding the identification of the Subject Accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
4. All available IP history related to the Subject Account(s);
5. The types of service utilized;
6. All records or other information stored by an individual using the Google accounts, including address books, contact and buddy lists, calendar data, pictures, videos and files. In addition, please provide the photos and videos in their original file format, including EXIF information;

7. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken;

8. All Google chat archives stored on servers controlled by Google;

9. All privacy settings and other account settings; and

10. All records pertaining to any Circles in which the Google accounts listed in Attachment A participated, including communications and content shared with other individuals within such Circles, the other individuals within those Circles, and the account/subscriber information of the other individuals within those Circles.

II. Information to be seized by the United States

All information described above in Section I, including correspondence, records, documents, photographs, videos, electronic mail, chat logs, and electronic messages, that constitutes evidence of a crime, contraband, fruits of crime, or other items illegally possessed, or property designed for use, intended for use, or used in committing violations of 18 U.S.C. § 1832, including, for each account or identifier listed on Attachment A, information pertaining to the following matters, including attempting and conspiring to engage in the following matters:

1. Credit card and other financial information including but not limited to bills and payment records;

2. The identity of the person(s) who created or used the Subject Accounts, including records that help reveal the whereabouts of such person(s);

3. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

4. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

5. Passwords and encryption keys, and other access information that may be necessary to access the account(s) or identifier(s) listed in Attachment B and other associated accounts;

6. The identity of the person(s) who communicated with the user ID about matters relating to exosomes, GENEXOSOME TECH, BEIJING

GENEXOSOME, and/or AVALON, including records that help reveal their whereabouts.